

**ORIGINAL**

1 KARL J. KRAMER (No. 136433)  
 JANA G. GOLD (No. 154246)  
 2 MORRISON & FOERSTER LLP  
 755 Page Mill Road  
 3 Palo Alto, California 94304-1018  
 Telephone: (415)813-5600  
 4  
 5 RAOUL D. KENNEDY (No. 40892)  
 MORRISON & FOERSTER LLP  
 345 California Street  
 6 San Francisco, California 94104-2675  
 Telephone: (415) 677-7000  
 7  
 8 PATRICK J. FLINN (No. 104423)  
 ALSTON & BIRD  
 One Atlantic Center  
 9 1201 W. Peachtree Street  
 Atlanta, Georgia 30306  
 10 Telephone: (404)881-7000  
 11 Attorneys for Defendants/Counter-  
 Claimants CYLINK CORPORATION, CARO-KANN  
 12 CORPORATION and STANFORD UNIVERSITY

13 UNITED STATES DISTRICT COURT  
 14 NORTHERN DISTRICT OF CALIFORNIA  
 15

16 ROGER SCHLAFLY,

17 Plaintiff,

18 v.

19 PUBLIC KEY PARTNERS AND RSA DATA  
 SECURITY, INC.,

20 Defendants,  
 21

22 RSA DATA SECURITY, INC.,

23 Plaintiff,

24 v.

25 CYLINK CORPORATION and CARO-KANN  
 CORPORATION, et al.

26 Defendants.  
 27

No. C-94-20512 SW

No. C-96-20094 SW

**NOTICE OF FILING  
 SUPPLEMENTAL DECLARATION IN  
 SUPPORT OF DIFFIE-HELLMAN  
 MOTION**

Date: September 4, 1996

Time: 10:00 a.m.

Courtroom: 4

Hon. Spencer Williams

28 NOTICE OF FILING SUPPLEMENTAL DECLARATION  
 IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT  
 ON DIFFIE-HELLMAN PATENT  
 C-96-20094 SW

120768

1 On July 31, 1996, defendants and counterclaim plaintiffs Cylink  
2 Corporation, Caro-Kann Corporation, and Stanford University  
3 ("defendants") filed a Motion for Summary Judgment on the Validity  
4 of the Diffie-Hellman Patent. Dr. Whitfield Diffie, one of the co-  
5 inventors of the patent, was unavailable to sign a declaration in  
6 support of that motion until August 1, 1996.

7 Defendants respectfully request that the Declaration of  
8 Whitfield Diffie, attached hereto, be considered in support of  
9 defendants Motion.

10 Dated: August 1, 1996

11 MORRISON & FOERSTER LLP  
12 ALSTON & BIRD

13  
14 By: 

Karl J. Kramer

15 Attorneys for Defendants/  
16 Counter-Claimants CYLINK  
17 CORPORATION, CARO-KANN  
18 CORPORATION and STANFORD  
19 UNIVERSITY  
20  
21  
22  
23  
24  
25  
26  
27

KARL J. KRAMER (Bar No. 136433)  
BRYAN WILSON (No. 138842)  
JANA G. GOLD (No. 154246)  
SHERMAN W. KAHN (No. 168924)  
Morrison & Foerster LLP  
755 Page Mill Road  
Palo Alto, California 94304-1018  
Telephone: (415) 813-5600  
Facsimile: (415) 494-0792

RAOUL D. KENNEDY (Bar No. 40892)  
Morrison & Foerster LLP  
345 California Street  
San Francisco, CA 94104-2675  
Telephone: (415) 677-7000  
Facsimile: (415) 677-7522

PATRICK J. FLINN (Bar No. 104423)  
ALSTON & BIRD  
One Atlantic Center  
1201 W. Peachtree Street  
Atlanta, GA 30306  
Telephone: (404) 881-7000  
Facsimile: (404) 881-7777

Attorneys for Defendants and  
Counter-Claimants CYLINK CORPORATION  
and CARO-KANN CORPORATION

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

RSA DATA SECURITY, INC., a  
Delaware Corporation,,

Plaintiff,

v.

CYLINK CORPORATION and CARO-KANN  
CORPORATION, a California  
Corporation, and THE BOARD OF  
TRUSTEES OF THE LELAND STANFORD  
JUNIOR UNIVERSITY,

Defendants.

AND RELATED COUNTER-CLAIMS

No. C-96-20094 SW(PVT)

**DECLARATION OF DR. WHITFIELD  
DIFFIE IN SUPPORT OF  
DEFENDANTS' MOTION FOR  
SUMMARY JUDGMENT ON THE  
VALIDITY OF THE DIFFIE-  
HELLMAN PATENT**

Date: September 4, 1996  
Time: 10:00 a.m.  
Courtroom: 4

The Hon. Spencer Williams

1 I, Dr. Whitfield Diffie, declare and state:

2 1. I am one of the named inventors on United States Patent  
3 No. 4,200,770 (the "Diffie-Hellman patent"). I am currently  
4 employed as a Distinguished Engineer at Sun Microsystems in Mountain  
5 View, California.

6 2. In late May or June, 1976, Dr. Hellman and I submitted a  
7 paper entitled "New Directions in Cryptography" to the IEEE for  
8 publication in the journal called Transactions on Information  
9 Theory. At the time we submitted the paper, we were aware that the  
10 paper would be circulated to a limited number of anonymous  
11 reviewers, who would be under an obligation to maintain the  
12 confidentiality of the paper. In approximately August, 1976, we  
13 revised the paper to incorporate changes suggested by the editors of  
14 the IEEE journal.

15 3. I have reviewed the Declaration of Peter Blatman,  
16 submitted to the Court by RSADSI in January, 1996. The paper  
17 attached to Mr. Blatman's declaration is a copy of the August, 1976  
18 version of the paper. I do not recall sending the paper to  
19 Mr. Blatman or anyone else in or around August, 1976. However, I do  
20 recall Mr. Blatman. Mr. Blatman was a graduate student at Berkeley  
21 in the mid-1970's, and it was through Mr. Blatman that I met Ralph  
22 Merkle, one of the coinventors of the Diffie-Hellman patent. Mr.  
23 Blatman and I both participated in a seminar given by Dr. Hellman at  
24 Stanford University during this period, and would commute from  
25 Berkeley to Stanford together. I considered Mr. Blatman a fairly  
26 close colleague at the time, and as such, it would have been my  
27 practice to share my academic work with him, and to seek his  
28 comments. It is common practice in academia to circulate such

1 papers prior to publication to ensure that any errors can be  
2 corrected. In my experience, it is widely understood that such  
3 papers are being sent in confidence. There is no question in my  
4 mind that Mr. Blatman would have understood that a paper such as the  
5 August draft of the "New Directions" paper was being sent in  
6 confidence, and that Mr. Blatman would not have circulated a paper I  
7 sent him without obtaining permission to do so.

8 4. In June, 1976, I attended the National Computer Conference  
9 in New York City, and gave an oral presentation covering some of the  
10 material in the "New Directions" paper. I also used slides at the  
11 National Computer Conference as a visual aid. However, I did not  
12 pass out copies of the slides. To the best of my recollection, I  
13 did not hand out or make available any copies of any draft of the  
14 "New Directions" paper at the National Computer Conference  
15 presentation.

16 5. In July, 1976, I was invited to give an afternoon seminar  
17 presentation to a small group of mathematicians at the IBM Watson  
18 Labs in Yorktown Heights, New York. I used slides in giving the  
19 seminar as a visual aid. However, I did not pass out copies of the  
20 slides. I discussed the subject matter of the "New Directions"  
21 paper at the IBM seminar. To the best of my recollection, I did not  
22 hand out or make available any copies of any draft of the "New  
23 Directions" paper at the IBM Watson Labs presentation.

24 I declare under penalty of perjury that the foregoing is true  
25 and correct. Executed this 1 day of August at Palo Alto,  
26 California.

27 Whitfield Diffie  
28 Whitfield Diffie